图书情报工作
第64卷 第12期 2020年6月

云服务协议引发的信息安全风险及图情机构的应对措施

■ 黄国彬[1] 郑霞[1] 王婷[2]
[1] 北京师范大学政府管理学院 北京 100875 [2]首都医科大学图书馆 北京 100069

摘 要：[目的/意义]云服务在图书馆的应用可有效提升图书馆的数据存储与计算能力，但也为图书馆带来众多信息资源安全问题，而云计算服务协议的不规范性更加剧了图书馆面临的信息安全风险。[方法/过程]选取8家云服务代表运营商的服务协议作为样本，聚焦云服务协议中有关信息安全的条款，从数据收集、数据存储、数据传输、数据访问和服务安全等5个方面深入分析当前云服务协议条款中存在的信息安全风险。[结果/结论]图书馆应用云服务可能面临的信息安全风险包括：云服务协议内容缺失，用户信息安全难以得到确切保护；云服务协议表述模糊，尚未建立健全的安全保障机制；云服务协议的制定更有利于云提供商，用户权利易受侵犯。在此环境下，图书馆应当进一步明确图书馆用户数据的所有权，强调图书馆信息资源的安全性。

关键词：云服务 服务协议 信息安全
分类号：G250.7
DOI：10.13266/j.issn.0252-3116.2020.12.005

1 引言

自2007年中国引入云计算以来，产业格局风起云涌，商业模式日趋融合，已然成为云服务行业技术发展的重要推力。据中国信息通信研究院最新发布的《云计算发展白皮书(2018年)》[1]统计数据显示，2017年中国云计算整体市场规模达到691.6亿元，增速34.32%，正处在高速增长阶段。尤其是近年来随着人工智能、大数据及“互联网+”等的积极推进，云计算技术正在向政务、金融、交通、工业、教育和医疗等领域加速渗透，推动我国各行业云计算技术应用朝着蓬勃发展、方兴未艾的关键时期不断迈进。在此背景下，将云服务应用到图书馆业务工作中已经成为大势所趋。随着发展与应用的深入，云计算为图书馆在软件环境、硬件存储、应用平台与服务方式等方面带来了深刻变革，与此同时也为图书馆带来众多安全问题，使图书馆数据资源的安全存储、知识产权保护、数据保密、用户权限管理和访问控制管理等受到威胁。

云服务协议是云服务提供商与图书馆在双方协商的基础上形成的服务契约，是代表云服务提供商可提供服务类型和服务方式的规范性说明文档。从服务协议的角度出发，分析其内容构成和基本模块，能够较为全面地反映现有云服务提供商可提供给图书馆的服务产品和基本模式，从中发现图书馆应用云服务面临的信息安全风险。鉴于此，笔者将对现有应用于图书馆的代表性云服务，就其涉及的服务协议进行内容分析，从中归纳出图书馆应用云服务产品可能引发的信息安全风险的类型和后果，并结合图书馆业务工作给出有针对性的应对措施，以期为图书馆管理者和用户在选择和操作云服务时提供参考与依据。

2 国内外研究综述

笔者于2019年9月以“云服务”并含“信息安全”为标题，通过CNKI、Web of Science等数据库检索相关文献，发现目前国内外围绕此课题的研究较少。其中，国内学者开展的相关研究主要可以分为以下几个方面：

(1)云服务平台信息安全体系的构建。如代田凤[2]在其研究中阐述了数据信息安全体系架构的三大原则，分别是：系统分级原则、创新性原则和资源整合原则，并在此基础上提出了构建计算机云服务数据信息安全体系的主要途径。此外，在政府信息公开的时

作者简介：黄国彬(ORCID:0000-0001-9059-8285)，副教授，博士，硕士生导师；郑霞(ORCID:0000-0002-9788-5823)，硕士研究生，通讯作者，E-mail:zhengxia199405@163.com；王婷(ORCID:0000-0001-5110-7893)，馆员，硕士。
收稿日期：2019-06-16 修回日期：2019-12-23 本文起止页码：38-48 本文责任编辑：徐健

代发展背景下,国内有较多学者基于云服务开展了政务数据信息安全体系建设的研究,较有代表性的如毕健欢[3]、陈洁[4]、刘琴[5]等,他们均认为在构建基于计算机云服务的政府政务数据信息安全体系的过程中,应当科学运用数据挖掘技术,设计完善的云服务技术模块,合理制定信息安全基础设施方案。

(2)云服务信息安全法律问题的研究。冀枫[6]认为,当前数字图书馆在建设云服务平台过程中,主要面临数据资源安全问题、版权问题、协议共享问题以及数据位置存放等问题,建议出台有针对性的政策法律,以加强图书馆信息资源的安全存储和管理,设置不同的登录权限和访问登记,从而确保图书馆信息资源服务的完整性和保密性。类似地,刘平、刘春[7]在其研究中指出,尽管云计算技术有效整合了图书馆信息资源,但也存在较多安全隐患,因此无论是对于图书馆还是云服务商,都应当尽可能保障信息资源的完整性和保密性,做好用户权限管理和访问控制。黄国彬、郑琳[8]则基于云服务提供的服务协议,从隐私政策、免责声明、协议终止和法律适用4个角度剖析了云服务协议的信息安全责任问题。

与国内学者相比,国外研究成果多集中于应用实证研究方法探索云服务环境下引发信息安全问题的风险因素及应对措施。S. T. Park 等[9]将安全风险因素分为信息泄露风险、故障恢复风险、合规风险和服务中断风险,并从这 4 个因素对持续采用意愿的影响进行了实证分析;类似地,S. K. Madria[10]认为,现阶段阻碍云服务发展的关键因素在于云服务提供商提供数据的安全性,可能存在数据存储、数据复制、完整性验证、访问控制、风险评估和安全查询处理等问题。对此,A. N. Kang [11]提出,应当利用云服务加强企业信息安全的方案,且方案的顺利执行需要得到政策和技术的双重支持。T. Halabi[12]设计了一种基于云安全的服务性能量化评估方法,并通过将其应用于 3 家云服务提供商验证了该方法的适用性和评价结果的有效性。

综合国内外现有研究成果可以发现,当前针对云服务引发的信息安全风险问题尚未得到学术界的广泛关注,较多学者聚焦于云服务信息安全体系的建设方案和实施策略,或依据实践经验总结云服务引发的信息安全风险类型,而从更能代表云服务商服务准则的规范性文档,即从云服务协议的角度剖析其引发信息安全风险的研究成果仍较为少见。当前,由于云计算技术的引入,图书馆大量的信息资源已不在自己手中掌握,而是挂到了“云端”,对数字信息资源的安全性和保密性造成极大威胁。基于此,笔者以应用于图书馆的云服务涉及的服务协议为基础进行内容分析,从中发现图书馆面临的云服务信息安全风险。

3　研究方法与数据来源

考察云计算环境下图书馆可提供的各类信息服务以及可能涉及的信息安全问题,需要系统调研云服务应用于图书馆所涉及的产品类型与业务领域。当前可应用于图书馆的云服务,既有适用于其他行业的、通用的云服务,也有结合图书馆业务特质而专门适用于图书馆的专用云服务。其中,通用云服务是指面向各个行业需求而设计的标准化云服务产品;而图书馆专用云服务是面向图书馆业务需求而设计的云服务产品,其主要功能包括托管图书馆管理系统、发现服务、在线数据库和统计分析工具。笔者全面调研了目前广泛应用于图书馆业务工作的通用云服务和专用云服务产品及其所在的图书馆名称,结果如表 1 所示:

表 1　图书馆应用主要云服务的现状

云服务类型	云服务提供商	云产品	代表性使用馆列举
通用云服务	Google	Google Cloud Platform	科罗拉多西部州立学院图书馆[13]、根特大学图书馆[14]、东肯塔基大学图书馆[15]等
	Amazon	Amazon Web Service	美国纽约公共图书馆[16]、美国俄亥俄州图书馆[17]、约克大学图书馆[18]等
	Microsoft	Windows Azure[19]	美国国会图书馆、美国马里兰大学图书馆等
	DuraSpace	DuraCloud[20]	美国国会图书馆、麻省理工学院图书馆、克利夫兰公共图书馆、佐治亚理工学院图书馆、都柏林大学图书馆等
专用云服务[21]	OCLC	WorldShare Management Services	伯明翰大学图书馆、特温特大学图书馆、曼尼克斯图书馆麦吉尔大学图书馆、乌得勒支大学图书馆、阿联酋大学图书馆等
	Ex Libris	Alma	剑桥大学图书馆、富勒顿大学图书馆、美国奥兰治海岸学院、旧金山城市学院图书馆、塞拉利昂大学图书馆等
	Biblionix	Biblionix Apollo	麦克布莱德纪念图书馆、费城 - 尼舒巴郡图书馆、萨拉多公共图书馆等
	Innovative Interfaces	Sierra	加州大学东海岸分校图书馆、澳大利亚国立大学图书馆、华中科技大学图书馆等

4 应用于图书馆的云提供商服务协议文本分析

通过对应用于图书馆的云计算服务代表运营商的隐私政策和服务条款的内容进行解读,笔者从云服务过程的数据管理生命周期,即数据收集、数据存储、数据传输、数据访问和服务安全等 5 个角度出发,设计了如表 2 所示的“云服务协议的核心内容概览”,对本研究选择的应用于图书馆的 8 家代表性云服务提供商服务协议进行文本分析,从总体上揭示图书馆面临的信息安全风险。

表 2 云服务协议的核心内容概览

数据生命周期	服务协议内容 \ 云提供商	Google[22]	Amazon[23]	Microsoft[24]	DuraSpace[25]	OCLC[26]	Ex Libris[27]	Biblionix[28]	Innovative Interfaces[29]
数据收集	收集内容	√	√			√	√	√	√
	收集目的		√			√	√	√	√
	收集途径					√	√		√
数据存储	存储位置	√	√						
	数据安全	√	√	√		√	√	√	√
	数据保留与删除		√	√		√	√	√	√
数据传输	加密传输		√						
	传输故障	√				√			
数据访问	访问主体	√	√						
	访问限制	√	√	√	√		√	√	√
服务安全	服务中断	√	√	√		√			
	服务终止	√	√			√		√	
	协议更改	√	√	√		√	√		
	免责声明与责任限制	√	√	√	√	√	√	√	√

注:“√”表示云服务商提供的服务协议涉及到该核心内容

4.1 数据收集

数据收集阶段涉及的云提供商服务协议意在明确云提供商拟收集用户数据的具体内容、收集数据的主要目的和收集数据时所采用的手段或方式等。总的来说,现有云服务协议中对于数据收集阶段的信息安全说明主要包括收集内容、收集目的和收集途径等 3 个方面。

(1)收集内容。通过分析现有云服务提供商提供的服务协议可以发现,云提供商收集的用户数据主要包括两种类型:一是包含用户个人数据的身份识别信息,如姓名、账号、密码、证件信息和联系方式等;二是用户使用云服务提供商提供的服务产品后生成的使用痕迹数据,如位置信息、设备信息或产生的其他日志数据等。如 Amazon 在其服务协议中指出,所收集的用户数据包括:用户提供给 Amazon 的个人数据信息、用户使用产品时自动生成的特定类型数据信息以及其他来源(如服务提供商、第三方合作伙伴或公开来源)的信息。OCLC 则规定,其并不强制收集用户信息,而是由用户自愿选择是否将其个人数据提交至服务平台,如若用户选择不共享其个人数据,则 OCLC 就无法提供更具个性化的服务应用程序。Ex Libris 和 Innovative interfaces 这 2 家云服务提供商也在其服务协议中也做出了与 OCLC 相同的规定。此外,OCLC 还规定了其收集用户个人信息的明细,包括用户账户信息、个人资料信息、专业背景信息、通信信息、用户生成内容、设备和浏览器信息以及使用信息和交易记录等。而 Biblionix 指出:“除图书馆客户端提供给我们的数据外,我们不收集或维护任何其他数据,包括用户直接或间接产生的任何更新、添加或修改的信息等”。

(2)收集目的。收集目的是指云服务提供商收集得到用户数据后,根据其自身需要,借助相关软件或第三方实现的目标或结果。现有云服务提供商中,Amazon、OCLC、Ex Libris、Biblionix 以及 Innovative interfaces 等 5 家云服务商均在其服务协议中对收集目的做出了说明。概括来看,数据收集的目的主要包括以下 4 种类型:①服务或产品必需;②改进服务或产品;③营销或广告投放;④其他目的。如 Amazon 规定:“我们使用您的个人信息来操作、提供和改进 Amazon 产品,如完成 Amazon 服务、改进或评估 Amazon 产品、识别用户偏好并提供个性化产品,以及履行法律义务等”。类似

地,Innovative interfaces 将通过收集用户个人信息用于为用户提供所需信息、帮助用户报名参加研讨会或学术交流活动、向用户发送其感兴趣的主题内容、通讯信息或产品服务、统计和识别网络访问者从而分析用户行为等。同时,OCLC 补充提出,得到用户数据之后,OCLC 可能与其他第三方服务提供商共享用户数据,包括云提供商合作组织、社交媒体平台、OCLC 其他附属机构和国家级图书馆等,在共享用户数据过程中将遵循数据合理使用规则,并运用可靠的安全技术保护用户个人信息不被泄露。

(3)收集途径。现有云服务提供商中,仅 OCLC、Ex Libris 以及 Innovative interfaces 这 3 家云服务提供商对收集用户信息的途径做出了说明。如 OCLC 指出,其收集用户资料的途径主要包括:通过用户与 OCLC 及其下属机构进行交互时收集信息、通过用户的计算机或 Web 浏览器收集信息、通过用户授权第三方机构共享而获得信息或由用户主动共享来获取信息。Ex Libris 主要通过 3 种方式收集用户信息:用户注册时收集信息、云提供商使用技术手段自动收集用户信息、通过第三方机构收集用户信息。

4.2 数据存储

数据存储阶段所涉及的应用于图书馆的云提供商服务协议意在为用户提供有关其数据存储位置、格式以及安全性等问题,以确保用户存储的数据具有高度的可靠性和透明性。总的来说,现有云服务协议中对于数据存储阶段的信息安全声明主要包括存储位置、数据安全、数据保留与删除等 3 个方面。

(1)存储位置。在云计算环境下,用户对于数据存储的物理地址并不清楚,用户数据有可能被服务提供商转移至别的国家或地区,也有可能同时存储于多个国家或地区,这将导致用户面临不同司法管辖体系争议的问题,因此有必要通过分析云服务协议中关于数据存储位置的相关条款,了解其所蕴含的数据安全风险。

现有云服务提供商中,Google、Amazon 和 Microsoft 这 3 家云服务代表运营商在其服务协议中就数据的存储位置进行了明确规定,提出用户可自行选择拟存储的数据类型、位置和地理区域,若用户未设置数据存储位置,则云服务提供商将根据实际情况自动存储用户数据内容。其中,Microsoft 公司在协议中明确指出用户数据可能会存储或转移到其他国家或地区,即规定:“通过 Microsoft 站点和服务收集的个人信息可能在 Microsoft 总部,或分公司、附属公司所在的任何国家或地区进行存储和处理”。这显然会使用户数据面临多个司法管辖区如何协调管理的问题,且各个国家或地区法律体系不尽相同,法律保护级别的差异也会加剧用户的信息安全风险。相对来说,Amazon 的规定更为人性化,其在用户服务协议的 3.2 节规定:“您可以自行设定个人数据存储的地区,我们不会在未经许可的情况下擅自将您的数据转移至别的国家或地区,除非需要遵守法律或政府请求”。这样一来,用户就可以根据自身需求选择不同法律保护级别的存储地区。但是,对于必须转移用户数据存储位置的情况,有关通知的形式和时间等细节并未在 Amazon 协议中明确提出。

(2)数据安全。在云计算环境下,数据存储的位置从本地磁盘转移到网络上。这意味着用户不是数据的唯一拥有者,服务提供商也拥有这些数据。这会给用户带来很大的不安全感。尤其对于图书馆用户而言,一旦将数据存储到“云端”,包括自身和图书馆在内,就已经不是事实上的数据拥有者和数据处理者,云服务提供商拥有甚至超过图书馆用户的权限,一旦这些权限失控,就会影响到图书馆用户的数据隐私。

笔者选择的 8 个分析样本中,除 DuraCloud 外,其余 7 家云服务提供商均在其服务协议中提及了数据安全的相关规定。概括来说,云服务商应当为数据提供物理安全措施和技术安全措施,具体来说:①物理安全措施。物理安全措施是指通过物理隔离实现对设备、设施的安全保护。如 Google 在其服务协议中提出:“用于存储和处理用户数据的设备设施都需要遵循安全标准,提高用户数据的安全性和机密性,防止用户信息遭到不必要的威胁而降低数据的完整性,不得使用未经授权的设施或应用程序访问和存储用户数据”。②技术安全措施。技术安全措施指的是借助数字化加密技术实现对用户账号或关联密码的保护,如密钥服务、权限管理和防火墙技术等。如 Amazon 提供了存储数据加密功能以及灵活的密钥管理选项,用户可选择自行控制存储内容或交由 Amazon 代理保障数据安全。此外,OCLC 和 Ex Libris 等均设置了用户数据安全保障程序,以防止未经授权而非法查阅、披露、更改、销毁或处理用户数据。

需要注意的是,尽管云服务提供商提供的服务协议中大多涉及了数据安全的相关规定,但并没有细化到具体的保护方案,仅是概括性的规定。其中,Biblionix 和 Innovative interfaces 这 2 家云服务提供商在其服务协议中明确指出,并不能保障用户存储的数据绝对安全,且未提及意外事件导致数据丢失或删除的处理

方案。这对用户存储内容带来较大的安全风险。

（3）数据保留与删除。在云计算模式下，图书馆各种类型的数据被随机存储在不同物理位置的各个虚拟数据中心，造成用户对其个人数据的控制权随之减弱，即使是用户删除数据后，有些服务提供商仍可能保留这些数据的副本，这在很大程度上增加了用户隐私权被侵犯的风险。因此，有必要进一步分析现有云服务提供商在其服务协议中提及的数据保留和删除的相关规定。

本研究选择的 8 个研究样本中，除 Google 和 DuraCloud 外，其余 6 家云服务提供商均提供了数据保存和删除的相关说明。从数据删除的维度来看，现有云服务提供商均指出，用户可随时保留或删除个人信息。如 Microsoft 在其服务协议中提出："当用户订阅服务过期或服务终止时，我们将继续保留您至少 90 天的客户数据，以便您可以提取；而在免费试用服务功能中，我们可以立即删除客户数据，无保留期限"。而部分云提供商并未说明数据保留或删除的时间期限，如 OCLC 指出："我们将根据服务协议规定保留您的信息，并遵照法律规则执行存储内容监管义务。如若存储内容不再适用法律效力，我们将销毁或删除用户信息，或将其转化成匿名形式继续保留。"此外，Amazon 虽然也在其服务协议中提到，会在用户注销账户后按用户要求删除信息，但是对数据是否能彻底删除、公司的服务器会不会仍然保留用户数据等问题没有做出确切说明。这无疑使得用户面临着隐私权的侵权风险。类似地，Biblionix 在其服务协议中明确提出："为保障图书馆信息系统的正常运行，Biblionix 将对所有数据信息（包括用户数据）进行多次备份，即使用户存储的数据已从仓储库中删除，也不能全部删除备份在系统后台存储媒体中的全部数据。不过，所有存储在存储设备中的备份信息都会得到加密保护"。

4.3 数据传输

数据传输阶段所涉及的应用于图书馆的云提供商服务协议意在明确，数据的传输过程是否受到了加密保护，以确保其传输内容安全可靠；信息传输过程中可能受到哪些不可抗力的威胁而造成传输故障；信息传输目标和对象，以及用户在信息传输过程中所拥有的知情权和控制权等。现有云服务协议中对于数据存储阶段的信息安全说明包括加密传输和传输故障两个方面。

（1）加密传输。在加密传输方面，现有云服务提供商中仅 Amazon 在其服务协议中明确提出："将用户数据传输到 Amazon 网站、应用程序和其他服务平台时，我们将使用加密协议和软件以确保信息传输的安全性"。而其他 7 家云服务提供商并未对数据加密传输拟采用的技术做出说明。然而，即便云服务运营商采用了加密技术，也只能保证数据在传输过程中处于加密状态，而存储和处理数据时，极易发生其他服务商或业务合作商访问用户数据引发安全问题，更加剧了用户信息泄露的风险。

（2）传输故障。云服务协议中提及的有关数据传输故障可以分为两种类型：一是由于计算机系统、软硬件等损害引发的故障；二是受到病毒、蠕虫感染等引发的数据传输故障。此外，不同云服务提供商对于因不可抗力造成传输故障而未能履行或延迟履行服务协议的情况也做出了说明。需要指出的是，云服务提供商均未说明由于上述原因导致数据传输故障的解决方式，默认由用户自行承担信息安全风险。如 Google 在其服务协议中指出："服务提供商和用户均无需对由于不可抗力造成的无法履行或迟延履行协议内容承担责任"；OCLC 指出："当发生火灾、爆炸和通信故障等无法控制的事故时，用户和云服务供应商无需对任何无法履行或迟延履行协议内容承担责任"；Amazon 规定："如若由于各类无法控制的因素（如天灾、劳资纠纷、公用设备故障、地震、暴风雨等）导致我们延迟或未能履行协议规定的任何义务，我们及我们的服务关联方均不对此承担任何责任"。

黑客、病毒等是威胁云计算时代网络信息安全的致命因素。"云"服务高度整合着各类型各地域图书馆的数字化资源，且云环境非常复杂，这大大增加了黑客利用云环境下的安全漏洞来窃取或滥用图书馆数据的机会，甚至还会迅速扩散到与"云计算"系统相联接的其他用户的计算机系统，进而造成更大损失。除了黑客、病毒等带来的安全风险，硬件系统也有可能造成信息失密，如计算机内的信息可能通过电磁波形式泄漏出去，外部网络通信线路也可能被截获、监听等。

4.4 数据访问

用户将数据上传到云端，会直接导致其对数据的掌控力弱化。在云服务模式下，用户不再是数据的唯一访问者，云服务公司的员工和合作伙伴都有可能对用户数据进行访问，且如果企业涉及合并、收购等交易时，可能会将用户的数据作为个人资产进行转移，这使得与该企业交易的公司也有权访问用户数据，从而加大用户数据泄露的风险。数据访问阶段所涉及的应用于图书馆的云提供商服务协议意在明确数据访问的主

体、使用方法,以及使用过程中可能存在的服务中断或终止、相应的救援措施等。从当前情况看,云服务协议中对于数据存储阶段的信息安全说明涉及访问主体和访问限制两个方面。

(1)访问主体。在云服务协议中,对于访问主体的规定意在说明有权访问用户数据或服务产品内容的个人或组织。明确不同应用场景下访问主体的权限对用户存储信息的隐私安全具有重要意义。根据现有云服务提供商提供的云服务协议,可将数据内容的访问主体分为3种类型,包括用户、云提供商和第三方机构。如Amazon在其服务协议中规定,用户可依照服务协议访问并使用服务产品,在访问过程中应当遵守服务协议的条款以及所有的法律法规;也指出“除为提供用户要求的服务所必需,以及受到相关法律法规要求,Amazon不会随意访问或使用用户数据,或将用户数据披露给任何第三方”。Microsoft指出,“我们不允许第三方机构(包括执法机构、政府机构或民事诉讼当事人等)访问用户数据,如遇特殊情况需要披露用户数据,我们将立即通知用户提供数据副本”。

但与此同时,云服务提供商提供的服务协议中并未提及对访问者身份的管理和验证措施,致使图书馆面临因云服务提供在访问者身份管理、访问控制和用户权限等方面的不明确性而遭遇信息安全问题。在云计算模式下,图书馆不再是数据的唯一拥有者,云服务提供商往往也拥有相同的数据。在受到某种经济利益或政治目的的驱使下,一些云服务提供商有可能会以图书馆未知的方式未经授权访问图书馆存储在云服务商相关系统中的数据,侵犯图书馆用户的隐私,给图书馆带来无可挽回的后果,且“云端”的数据处于高度共享的环境中,如果缺乏合理的用户访问控制,缺乏对信息操作权限的有效管理,很大程度上会导致图书馆的数据被非法访问。

(2)访问限制。访问限制指的是在数据访问阶段对数据的访问过程、方式及后续使用的合理限制,其是保障用户合法履行信息限制条款的基础和依据,对用户确保数据访问过程中信息安全和个人隐私具有重要意义。具体来说,访问限制包括使用权利、许可限制以及版权政策等内容:①从使用权利来看,Google提出:“除需要为用户提供必要服务,我们不会随意访问或使用用户数据”。②从知识产权来看,现有云服务提供商大多对版权政策提出了较为详细的规定。如Google提出其拥有对云端服务和所有软件的知识产权,而对于用户数据版权问题的处理将遵循《数字千年版权法》,并帮助版权所有者在线实时管理其知识产权。同时,如若用户认为他人侵犯了其知识产权,可以随时通过Google官网提交相关申诉说明,以寻求Google后台帮助。Amazon提供了较为详细的知识产权相关规定,要求用户务必遵守服务协议所规定的限制条件。如若发生知识产权纠纷,需由用户对此负责。DuraCloud指出将为用户授予永久的、全球性的、非排他性的、免费的版权许可,用于版权作品的复制、展示、公开或再传播等。Ex Libris、Biblionix以及Innovative interfaces这3家云服务提供商均提出,其网站全部内容(包括文字、图像、徽标等)均受到版权保护,未经网站许可,任何主体不得任意访问、修改或复制服务内容。③从服务产品许可来看,Amazon授予用户一项有限的、非排他性的、可撤销的、不可转让的使用许可,用户在访问和使用云服务商提供的服务时必须遵循该协议规定,而不得获取服务产品的知识产权。

4.5 服务安全

除上述模块外,现有云服务提供商还在其服务协议中对服务安全做出了相关规定。云服务协议提及的服务安全意在说明服务商在提供服务的过程中如何保障用户信息安全、如何处理意外事件发生而造成的数据丢失或删除情况,此外还包含运营商对其责任履行的免责声明或责任限制等。

(1)服务中断。云计算是一种基于Internet的计算模式,对网络的依赖程度非常强。现有云服务提供商提供的绝大多数服务协议规定,如若用户发布的内容或其操作行为违反了合理使用规则,则云服务提供商将在规定时间内告知用户,要求其纠正违规行为,或暂停用户使用云服务产品的部分或全部功能。如Google规定:“如果用户未能在Google要求的24小时内纠正违规行为,则Google可以暂停用户使用本产品的部分或全部功能”。而OCLC对服务中断的规定较为模糊,其指出:“若用户存在严重的违反本条款行为,OCLC将立即采取措施暂停用户访问WorldShare平台”,但此协议对于“违反条款的行为”并未给出清晰的界定,这无疑给予该服务提供商较大的自由裁量权。

除上述云服务使用者违规使用服务产品而导致服务中断之外,在业务实践中,停电、地震等突发性事件,或软件故障、硬件老化、人为操作失误等都有可能造成网络故障。一旦发生网络故障,将会造成云计算服务中断,图书馆将无法借助云服务开展工作。同时,若云计算服务商破产或被他人收购,也会造成服务中断或不稳定。服务安全方面还包括服务协议的合法性,在

云计算模式下,一些云服务提供商为图书馆提供的服务内容有可能与服务协议不完全相符。一旦运营商要停止某项服务,用户因未接到通知而无法提前转移自己的数据,这也会给图书馆带来安全风险。

(2)服务终止。与服务中断的相关规定类似,现有云服务提供商提供的多数服务协议也提出,如若用户的操作行为违反了服务协议,服务提供商将终止用户使用部分或全部服务或项目。此外,Google 还补充提出其他可能导致服务终止的情况,具体包括:①用户在60天内未使用云服务平台或没有其他网络活动,且Google 提前30天通知用户仍未应答,Google 将终止用户使用 Google 服务产品的权利;②为方便管理,用户或 Google 均可随时终止服务协议,且 Google 无需向用户承担任何责任。而 OCLC 对服务终止的规定更加强调从自身情况出发,其提出:"OCLC 可以在任何时间、以任何原因部分或完全终止用户使用 WorldShare 平台,且无需承担任何责任",类似地,Biblionix 提出:"Biblionix 可以在任何时候、以任何原因提前120天给用户发送书面通知,说明服务终止"。

而对于服务终止的结果,不同云服务提供商也对此做出了不同说明。如 Google 提出,若服务终止,则其将归还或删除用户存储在云服务器端的全部数据;类似地,Biblionix 也提出:"Biblionix 应及时删除或以其他方式销毁其拥有或控制的所有用户数据"。而 Amazon 则规定:"我们不会因服务终止而移除用户存储在 Amazon 系统中的任何数据"。

(3)协议更改。现有云服务提供商提供的服务协议通常规定,如若服务协议发生更新或修改,云服务提供商应当及时通过用户个人账户或电子邮箱向其发送协议更改说明,并鼓励用户采取必要的保护措施防止个人信息丢失或被删除。但不同云提供商对于预先通知时间的说明各不相同,如 Amazon 和 Google 均规定,若服务商对服务协议进行了修改,则应当至少提前90日向用户发出通知;Microsoft 规定:"我们可能不定时更改服务协议。除非出于安全、法律或系统性能等方面的考虑需要尽快删除用户数据,否则在更新或删除任何服务功能之前,我们将提前12个月通知您"。而 OCLC 和 Ex Libris 均在其服务协议中指出,云服务商可在任何时间自行更改服务条款,且通过为用户发送电子邮件或在服务平台网站发布服务变更公告等形式告知用户。

(4)免责声明与责任限制。免责声明旨在明晰云服务商在何种情况下无需对未履行服务协议内容的行为承担责任,而责任限制则规定了在特定情况下对云服务提供商和用户责任范围进行限制的法律手段。分析发现,现有云服务提供商提供的服务协议中均对免责声明和责任限制做出了较为细致的规定。其中,对于免责声明的共性要求是:除服务协议中明确规定的款项外,用户应当对违反服务协议而产生的任何损失负责,云服务提供商不对此承担任何责任。如 DuraCloud 规定:"除本服务协议说明外,我们不提供任何明示、暗示或其他保证,包括适销性或适合特定用途的保证"。

同时,部分云服务提供商在其服务协议中对于责任限制提出了详细说明,如 Google 从间接责任限制、责任限额和责任限制例外等3个部分阐述了责任限制的具体实施方案。其中,间接责任限制要求:"在法律允许的情况下,Google 供应商和用户都将根据本协议承担损失或间接赔偿";责任限额要求:"在法律允许的情况下,用户不得在导致责任事件发生的前12个月内,向 Google 支付超过额定责任款项的金额";责任限制例外要求:"上述责任限制不适用于一方侵犯另一方的知识产权、赔偿义务或客户的付款义务等情况"。Biblionix 指出:"在任何情况下,Biblionix 均无需对因本协议而产生的后续赔偿向用户承担责任"。

5 云服务协议引发的图书馆信息安全风险分析

5.1 云服务协议内容缺失,用户信息安全难以得到确切保障

根据上文分析可知,现有云服务协议存在表述模糊的问题,造成图书馆用户信息安全难以得到确切保障。从数据收集方面来看,尽管多数云服务提供商在其服务协议中明确提出了有关数据收集内容、收集目的和收集途径的规定,但并未清晰界定相关概念,比如,图书馆用户个人数据的概念范围。此外,部分运营商还将通过第三方服务平台收集用户个人数据,却未提及如何对其身份进行安全识别和认证,造成不同运营商在实际收集用户个人数据时有较大的自由空间,对用户个人信息安全带来较大潜在的威胁。从数据存储方面看,大部分云服务运营商似乎并不认为需要就用户数据的存储位置和转移情况进行说明,用户数据的存放或转移完全由云服务运营商自行决定。这将导致服务过程中用户对数据掌控能力的不断减弱,而且这种做法也违背了交易过程中应有的用户知情原则。

更重要的是,数据的存储和迁移关系到纠纷发生时的法律适用问题,随意将用户数据存储于其他国家或地区会大大加重使用云计算国际服务的用户的法律责任风险。

从数据传输方面看,目前大多数云服务提供商并未在其服务协议中提出在数据传输过程中是否采用了加密技术或安全标准。此外,在云服务协议中强调应用多种手段确保数据传输过程中的数据安全,但仍将计算机系统、硬件或软件损害及其他性能故障、病毒、蠕虫感染等应由云服务运营商承担责任的情况纳入到免责声明当中,强调一旦发生上述情况,云服务运营商不必承担责任,而由用户自担风险。这对用户来说是很不公平的。

从数据访问方面看,部分云服务协议对访问主体进行了控制,并且制定了相应的访问控制政策,但未提及如何对访问主体的身份进行认证,以及如果在数据访问过程中发生侵权行为应当遵照何种法律对此进行处理等问题。这就意味着在数据访问的过程中多数访问主体仍可以自由访问、利用甚至滥用图书馆数据,而无需对其行为负责。

综上可知,现有云服务协议内容规定不够全面,尚未提供信息安全问题的解决方案,在应对纷繁复杂的信息安全风险问题时略显无力,也使用户的信息安全难以得到确切保障。

5.2 云服务协议表述模糊,尚未建立健全安全保障措施

从云服务协议的表述方式来看,现有云服务提供商提供的云服务协议存在表述模糊的情况。从数据收集方面来看,云服务提供商在其服务协议中规定了收集用户数据的途径、目的等,但部分运营商在其服务协议中的收集目的的模块中声明,将与第三方机构共享用户数据,但这一行为的目的是用于改进服务或产品还是其他用途,云服务提供商并未对此做出确切说明。从数据存储方面来看,根据上述分析可知,当前云服务商提供的服务协议中对于数据删除的彻底性和时效性问题均进行了模糊处理,且部分云服务提供商还会对数据进行定期备份。也就是说,某读者通过图书馆使用的云服务,将存储在"云端"的个人数据被删掉之后仍可能通过备份恢复得到。这样一来,用户的隐私便得不到很好的保证。

从数据访问方面来看,现有云服务提供商在其服务协议中对访问主体和访问限制进行了说明,但其中仍存在表述含混的问题。如部分运营商规定:"如若遇特殊情况需要披露用户数据,将通知用户提供个人数据副本",但对于此情况下用户应当提供的个人数据的范围和程度,并没有给出明晰规定。

由此可见,现有云服务提供商拟定的服务协议存在表述模糊的问题,尤其是对于用户个人数据安全的保护范围界定不清,也尚未建立健全用户信息安全保障措施,加之大部分用户的信息安全意识还不够强烈,并未意识到云服务协议在信息安全风险责任认定中扮演的重要角色,因而很少有用户主动查证云服务协议是否存在表述缺失、歧义或模糊的问题。这就导致许多用户直接使用了云服务,却并不了解云服务协议的相关条款义务,从而在其信息安全遭受损失时无法向云服务运营商提出及时的、合理的赔偿。

5.3 云服务协议更有利于云提供商,用户权利易受侵犯

除上述分析外,现有云服务协议还存在更有利于云服务提供商的问题,导致权利的天平倾向于云服务提供商,而用户的合法权利更易受到威胁。这一问题主要体现在云服务协议中对于服务安全的规定。比如,从服务安全来看,绝大多数云服务协议都明确规定若由于服务中断、服务不及时导致用户的信息安全受到威胁,云服务运营商无需为此负责。并且,除少数云服务协议外,大多数云服务协议并未就服务终止进行说明。这意味着一旦云服务运营商在未通知用户的情况下单方面结束云服务进而导致用户数据损毁,云服务提供商也可以借口云服务协议未作相关规定而逃避责任。

从上述分析可知,当前云服务协议在对用户要求苛刻的同时,将几乎全部可能导致用户数据泄露及损毁等安全风险的情况都纳入到免责声明中,云服务协议的拟定更有利于服务商,造成用户的合法权利易受到威胁,进而在发生纠纷时凭借云服务协议独善其身。在服务协议中早已就可能出现的信息安全风险情况以及相应责任的分配进行了说明,而省略了与用户协商的过程。用户想要使用云服务,必须无条件接受云服务协议中的全部规定,否则将无法使用相应云服务。这就导致许多用户为了获得云服务的使用权而被迫放弃其他应有权利,进而增加自身的信息安全风险与责任。

6 图书馆应对云服务协议信息安全风险的策略

云服务协议是图书馆与云提供商之间有效沟通和

问题解决的契约。尽管不同的云服务提供商会提供不同的云服务协议内容,但是,图书馆在签订这类云服务协议时,不但要强调必备的内容模块,而且在具体内容的立场态度上,也要有明确的考虑。基于上述分析,笔者认为,图书馆在应用云服务提供商提供的服务产品时,应当采取如下措施应对云服务协议引发的信息安全风险:

6.1 明确图书馆用户数据的所有权

图书馆应确保其仍保有全部信息资源的所有权。图书馆信息资源包括传统信息资源、个人数据和虚拟化计算资源,而从其表现形式来看,图书馆信息资源主要包括全部文本、数值型数据、数据库记录、媒体文件、人口统计信息、检索历史、地理位置信息和元数据,或其他数据及信息,包括作为云计算服务用户的图书馆直接提供给云服务提供商的,或是云服务提供商因提供图书馆云服务而直接或间接访问获得的图书馆其他信息资源。如发生不利于云服务提供的数据使用行为,云服务提供商必须以及时、适当的方式告知图书馆。数据公开访问的前提包括:已获得数据所有者正式授权发布的数据授权书,或已提前通知数据所有者,亦或已获得管辖数据的法庭出具的数据公开官方命令。在所有情况下,刑事司法信息的所有者必须被实时通知任何试图或已完成的对其数据的非法访问。

6.2 强调信息资源的完整性

图书馆需要确保信息资源的完整性,要求云服务提供商必须保持图书馆信息资源的物理完整性与逻辑完整性,可考虑通过云存储与服务间的物理或逻辑分离实现这一目的。图书馆的信息资源不应该以任何损害数据完整性的方式存储、共享、处理或修改。如果云服务系统被设计用来储存图书馆所服务的个人数据,那么云服务提供商需要确保用户数据访问记录的完整性,并允许图书馆为具有较高隐私保护需求和知识产权保护诉求的信息资源建立一条监管链。在需要提取图书馆信息资源的操作记录时,云服务提供商还应协助图书馆建立监管链或其他与云相关的技术论证。在图书馆要求选择数据时,云服务提供商应通知图书馆相应操作是否,或是何时更改了数据的物理存储位置。

6.3 确保图书馆信息资源的保密性

云服务提供商应确保其代图书馆保存的信息资源的保密性。图书馆需要让云服务提供商,采取一切必要的物理、技术、管理与程序措施以保护图书馆信息资源的保密性。这些措施可能包括物理安全措施、对访问权限的要求、对网络安全的要求、对可访问系统或数据的职员与外包商的犯罪历史背景安全检查、安全意识培训、加密、定期审计,以及地理位置限制。云服务提供商应提供相应的凭据,证明其具有技术和业务能力,能够对提供给图书馆的系统与服务的网络安全进行独立评估。云服务提供商应提供及时的、适当的文本以证实其目前拥有网络安全风险预警措施。此外,云服务协议还应表明云服务提供商认同在与图书馆合作期间持续维护此前所述的各项风险预防措施。

6.4 保证图书馆信息资源的可用性、可靠性和高性能

图书馆通过云服务提供商获得云服务后,需要确保信息资源的可用性、可靠性和高性能,应要求云服务提供商根据云服务协议约定的性能指标为图书馆提供云服务,并能够根据涉及业务的重要程度,要求云服务提供商提供相应等级的云服务。对于部分服务(如检索已存档的数据或电子邮件),较低水平的可用性与性能即可被接受,但对于更为关键的服务,如计算机辅助调度(Computer-Aided Dispatch),则需要更高水平的可用性与性能。

除此之外,负责签订云服务协议的图书馆员,需要仔细阅读云服务协议,以随时发现不利于维护图书馆信息安全的问题。通常情况下,在注册云服务时,一般个人用户不会仔细阅读云服务协议。即使阅读,也不会十分认真,多是点到即止的大致浏览。之所以出现这种情况,一方面是由于用户本身对云服务协议不够重视,没有认识到其中可能存在的信息安全风险。另一方面也与云服务提供商的刻意引导有关。通常,云服务协议主要有点击式和浏览式两种类型。点击式是指用户在注册时,需通过点击"我同意"才能完成注册的服务协议形式;阅览式是指用户需要主动阅读服务协议并单击进入相应界面浏览的服务协议形式。点击式服务协议具有较好的通知性,即能够在一定程度上起到提醒用户阅读服务协议的作用。而浏览式服务的通知性则较差,除非用户主动查找,否则直接默认用户已经阅读了服务协议并且没有丝毫异议。并且,浏览式服务通常将链入服务协议内容页面的按钮设置在网页最不明显的位置,更易导致用户对服务协议的忽视。

当然,这两种协议都属于格式协议。对于图书馆而言,应用小规模的云服务,可以考虑直接接受这类格式协议;而一旦所签订的云服务协议,其影响涉及更大的业务范围、覆盖更多的图书馆信息资源,或者是更为敏感的个人数据时,图书馆则不应该直接接受这类格式协议,而应该通过商讨的方式,逐条确认后再签订云

服务协议。对于这类云服务协议,从起草、修改到定稿,负责签订协议的图书馆员都应该严谨把好协议的内容关。

7 结语

近年来,云服务在图书馆的应用深刻影响了图书馆的运作方式和服务模式,也为传统图书馆及数字图书馆构建了新的应用场景。目前,以 OCLC、美国国会图书馆、英国国家图书馆、JISC 和中国 CALIS 等为代表的国内外图书馆机构已开启了云计算在图书馆的应用实践。然而云服务的引入也为图书馆带来了诸多问题,其中之一便是易引发信息安全风险。尽管现有云服务提供商在其服务协议中对可能出现的信息安全风险情况及相应责任分配问题进行了说明,但却省略了与用户协商或协调解决的过程。如若图书馆用户想要使用云服务产品,就必须无条件接受云服务协议中的全部规定,而自主选择的空间较小。这就导致用户为了获取云服务使用权而被迫放弃其他应有权利,进而增加了自身信息安全风险和所需承担的责任。这主要与现阶段云服务提供商的技术、管理水平还无法绝对保障用户信息安全,以及云服务用户数量过多,云服务提供商无法与用户一对一协商拟定服务协议有关。

笔者选择了当前应用于图书馆的 8 家较有代表性的云服务提供商提供的服务协议作为分析对象,从可能引发图书馆信息安全风险的角度对其内容进行了剖析,并基于此提出有针对性的解决方案。需要指出的是,当前国内外对应用于图书馆的云服务可能带来的安全问题关注程度并不高。要使图书馆更加放心大胆地使用云服务,促进云计算更好更快地发展,不仅需要云服务提供商从技术的角度使得云服务安全威胁行为“想为而不能为”,为图书馆数据和服务提供充分地安全保障;还需要立法界通过制定严格的法律使得云服务安全威胁行为“能为而不敢为”。相信从技术和法律两个方面同时努力,在不久的将来,云服务提供商可以为图书馆及其他用户提供一片美丽的“蓝云”。

参考文献:

［1］中国通信院. 中国信通院发布 2018 年云计算发展白皮书——行业云时代全面开启［EB/OL］.［2019－08－26］. http://www. caict. ac. cn/kxyj/qwfb/bps/201808/t20180813_181718. htm.
［2］代田凤. 基于计算机云服务的数据信息安全体系构建［J］. 数字技术与应用,2017(11):188－190.
［3］毕健欢. 基于计算机云服务的政府政务数据信息安全体系创设研究［J］. 数字技术与应用,2016(2):203.
［4］陈洁. 基于计算机云服务的政府政务数据信息安全体系构建研究［J］. 山东工业技术,2016(3):116－117.
［5］刘琴. 基于计算机云服务的政务数据信息安全体系建设研究［J］. 中国管理信息化,2018,21(12):138－139.
［6］冀枫. 数字图书馆云服务平台的架构与信息安全探讨［J］. 内蒙古科技与经济,2018(20):49－51.
［7］刘平,刘春. 基于云服务的图书馆建设与信息安全策略研究［J］. 兰台世界,2015(8):126－127.
［8］黄国彬,郑琳. 基于服务协议的云服务提供商信息安全责任剖析［J］. 图书馆,2015(7):61－65.
［9］PARK S T, PARK E M, SEO J H, et al. Factors affecting the continuous use of cloud service: focused on security risks［J］. Cluster computing, 2016, 19(1):485－495.
［10］MADRIA S K. Security and risk assessment in the cloud［J］. Computer,2016, 49(9): 110－113.
［11］KANG A N, BAROLLI L, PARK J H, et al. A strengthening plan for enterprise information security based on cloud computing［J］. Cluster computing, 2014,17(3):703－710.
［12］HALABI T, BELLAICHE M. Towards quantification and evaluation of security of cloud service providers［J］ Journal of information security and applications, 2017, 33: 55－65.
［13］VASANTHA R N. Cloud computing for college library automation［EB/OL］.［2019－12－14］. https://www. slideshare. net/Vasanthrz/cloud-computing-for-college-library-automation.
［14］JUTA S. Digitizing and cataloging the Boekentoren［EB/OL］.［2019－12－15］. https://blog. ml6. eu/digitizing-and-cataloging-the-boekentoren-book-tower-ffc0070793ac.
［15］ZAINAB A, CHONG C, CHAW L. Moving a repository of scholarly content to a cloud［J］ Library Hi Tech, 2013, 31(2):201－215.
［16］AMAZON. New York Public Library's cloud journey［EB/OL］.［2019－12－16］. https://amazonAmazon-china. com/cn/blogs/enterprise-strategy/new-york-public-librarys-cloud-journey/.
［17］OSU. EDU. Ohio State AMAZON now includes enterprise support［EB/OL］.［2019－12－16］. https://it. osu. edu/news/2019/03/04/ohio-state-Amazon-now-includes-enterprise-support.
［18］Today in APIs: AMAZON Announces EC2 Spotathon［EB/OL］.［2019－12－16］. https://www. programmableweb. com/news/today-apis-Amazon-announces-ec2-spotathon-nasdaq-music-to-your-ears-and-11-new-apis/2012/11/09.
［19］Microsoft Azure［EB/OL］.［2019－12－17］. http://www. microsoft. com/windowsazure/.
［20］DuraSpace. DuraCloud［EB/OL］.［2019－12－17］. https://duraspace. org/duracloud/.
［21］Library technology guides［EB/OL］.［2019－12－18］. http://librarytechnology. org/.
［22］Google cloud platform agreement［EB/OL］.［2019－12－18］. https://cloud. google. com/terms/#google-cloud-platform-agreement.
［23］AMAZON customer agreement［EB/OL］.［2019－12－18］. ht-

tps://www. amazon. com/gp/help/customer/display. html? nodeId = 468496.
[24] Microsoft Azure legal information[EB/OL]. [2019 – 12 – 18]. https://azure. microsoft. com/en-au/support/legal/.
[25] License. DuraCloud [EB/OL]. [2019 – 12 – 18]. https://duraspace. org/duracloud/license/.
[26] OCLC. WorldShare platform terms and conditions[EB/OL]. [2019 – 12 – 18]. https://www. oclc. org/content/dam/developernetwork/PDFs/platform_general_TCs_0%20(1). pdf.
[27] Terms of Use. Ex Libris Knowledge Center[EB/OL]. [2019 – 12 – 18]. https://knowledge. exlibrisgroup. com/TERMS_OF_USE.
[28] Apollo integrated library system subscription purchase agreement. Biblionix[EB/OL]. [2019 – 12 – 18]. https://seguin. biblionix. com/agreements/subscription/? agreed = 2019-02-15% 2015% 3A45%3A27.
[29] Terms of Use. Innovative[EB/OL]. [2019 – 12 – 18]. https://www. iii. com/terms-of-use/.

作者贡献说明：
黄国彬：论文选题，论文撰写、修改与指导；
郑霞：论文的素材收集与整理，论文撰写与修改；
王婷：部分论文素材收集，论文初稿的撰写。

Information Security Risks Caused by Cloud Service Agreement and Suggestions for Library and Information Community

Huang Guobin[1] Zheng Xia[1] Wang Ting[2]
[1] School of Government, Beijing Normal University, Beijing 100875
[2] Capital Medical University Library, Beijing 100069

Abstract: [**Purpose/significance**] The application of cloud service in the library can effectively improve the data storage and computing capacity of the library, but it also brings a lot of information resource security problems, and the non-standard cloud computing service agreement aggravates the information security risks faced by the library. [**Method/process**] This paper focused on the information security clauses in the cloud service agreement, selected 8 cloud services on behalf of the operator's service agreement as a sample, and analyzed the information security risks that exist in the current cloud service agreement terms in depth from data collection, data storage, data transmission, data access and service security. [**Result/conclusion**] The information security risks that library application cloud services may face include: the lack of cloud service agreement content, the difficulty of obtaining accurate protection of user information security; the vague description of cloud service agreement, the establishment of a sound security guarantee mechanism; the formulation of cloud service agreement are more conducive to cloud providers, so user rights are vulnerable. In this environment, the library should further clarify the ownership of library user data and emphasize the security of library information resources.

Keywords: cloud service service agreement information security risk